Hybridization of Network Security and Performance as a Service

Enterprises have traditionally tried to address network performance and security challenges separately. But traffic growth from sources such as mobile devices and public cloud services is constraining enterprise networks; the problem is being magnified by the increasing size and frequency of attacks on network infrastructure. This report describes how these demands are shaping hybridization between on-premises, cloud-based security, and network and application performance services.

KEY FINDINGS

- Although hosted private cloud and public cloud are still in the early stages of adoption in large enterprises, companies expect to increase their use of various cloud services and will need to rethink the requirements for network performance and availability.
- Enterprises have plans for increased spending on Web application firewall (WAF) and DDoS services, but the attention and budget fall short of our expectations. Some roadblocks to overcome include: resistance to buying cloud-based security services; issues with who controls the overall IT budget process; and attention focused elsewhere because of matters such as integrating existing security solutions.
- Concerns about network and Web application security are becoming intertwined with content and Web application performance. Providing these formerly separate functions as services from the cloud can help increase both network performance and security while reducing complexity and management costs. This trend is manifesting itself in the marketplace through the combination of content delivery and cloud-based DDoS and WAF services from vendors.

FEB 2015

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

The terms of use regarding distribution, both internally and externally, shall be governed by the terms laid out in your Service Agreement with 451 Research and/or its Affiliates. The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such. 451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

451 Research®

New York
20 West 37th Street, 6th Floor
New York, NY 10018
Phone: 212.505.3030
Fax: 212.505.2630

London
Paxton House (5th floor), 30 Artillery Lane
London, E1 7LS, UK
Phone: +44 (0) 207 426 0219
Fax: +44 (0) 207 426 4698

San Francisco
140 Geary Street, 9th Floor
San Francisco, CA 94108
Phone: 415.989.1555
Fax: 415.989.1558

Boston
125 Broad Street, 4th Floor
Boston, MA 02109
Phone: 617.275.8818
Fax: 617.261.0688

TABLE OF CONTENTS

SECTION 1
Executive Summary

1.1 INTRODUCTION

Enterprises have taken to private and public cloud computing for the advantages in business agility that virtualization and on-demand business models offer. However, surveys conducted by 451 Research reveal that traffic growth from sources such as mobile devices and public cloud services is constraining enterprise networks. The capacity problem is being magnified by the increasing size and frequency of attacks on network infrastructure.

Enterprises have traditionally addressed network performance and security challenges separately. This report looks at spending trends in network and application security for signs of what lies ahead in the market. The market for distributed denial of service (DDoS) protection services, in particular, is an example of where there is growing interest in a hybrid of on-premises and cloud-based security.

We believe that over time, increasing use of hybrid and public cloud services for enterprise applications will help pave the way for growing use of other hybrid on-premises and cloud-based services. In particular, the sometimes conflicting demands for business agility, better network performance and better security are going to shape the melding of cloud-based security and cloud-based network and application performance services. This market evolution presents some challenges as well as opportunities for vendors and enterprises alike.

1.2 KEY FINDINGS

- Although hosted private cloud and public cloud are still in the early stages of adoption in large enterprises, companies expect to increase their use of various cloud services and will need to rethink the requirements for network performance and availability.
- Enterprises have plans for increased spending on Web application firewall (WAF) and DDoS services, but the attention and budget fall short of our expectations. Some roadblocks to overcome include: resistance to buying cloud-based security services; issues with who controls the overall IT budget process; and attention focused elsewhere because of matters such as integrating existing security solutions.
- Concerns about network and Web application security are becoming intertwined with content and Web application performance. Providing these formerly separate functions as services from the cloud can help increase both network performance and security while reducing complexity and management costs. This trend is manifesting itself in the marketplace through the combination of content delivery and cloud-based DDoS and WAF services from vendors.
- Enterprises should consider ways to augment protection from DDoS attacks at all layers by using cloud-based detection and mitigation services. Priority should be given to those vendors with a roadmap for integration with on-premises equipment, if vendors have not already implemented APIs.

- Security vendors need to ensure easier integration between on-premises and cloud-based services. Sometimes this might come in the form of a hosted service owned by the vendor, but the vendor must also be sure to consider channel conflicts with telcos, carriers and the like that may have already built services on its equipment.
- Network service providers (carriers, telcos and the like) need to consider partnering with vendors of DDoS mitigation services if they can't provide off-net services.
- Cloud service providers with partners for CDN services should consider extending these relationships to include security offerings.

1.3 METHODOLOGY

This report on the hybridization of network security and performance is based on a series of in-depth interviews with a variety of stakeholders in the industry, including technology vendors, managed service providers, telcos, VCs and IT managers at end-user organizations across multiple sectors. This research was supplemented by additional primary research, including attendance at a number of trade shows and industry events.

Reports such as this one represent a holistic perspective on key emerging markets in the enterprise IT space. These markets evolve quickly, though, so 451 Research offers additional services that provide critical marketplace updates. These updated reports and perspectives are presented on a daily basis via the company's core intelligence service, 451 Market Insight. Forward-looking M&A analysis and perspectives on strategic acquisitions and the liquidity environment for technology companies are also updated regularly via 451 Market Insight, which is backed by the industry-leading 451 M&A KnowledgeBase.

Emerging technologies and markets are also covered in additional 451 channels, including Datacenter Technologies; Storage; Enterprise Platforms & Infrastructure Software; Networking; Information Security; Data Platforms & Analytics; Development, DevOps & Middleware; Social Business Applications; Service Providers; Cloud & IT Service Markets; European Services; MTDC; Enterprise Mobility; and Mobile Telecom.

Beyond that, 451 Research has a robust set of quantitative insights covered in 451 products such as ChangeWave, TheInfoPro, Market Monitor, the M&A KnowledgeBase and the Datacenter KnowledgeBase.

All of these 451 services, which are accessible via the Web, provide critical and timely analysis specifically focused on the business of enterprise IT innovation.

This report was written by Jim Davis, Senior Analyst, Service Providers, with assistance from Adrian Sanabria, Senior Security Analyst and other members of the 451 Research team. Any questions about the methodology should be addressed to Jim Davis at: *jim.davis.@451research.com*.

For more information about 451 Research, please go to: *www.451research.com*.

SECTION 2

Market Trends

2.1 CLOUD IN THE ENTERPRISE PUSHES CHANGES IN NETWORKING

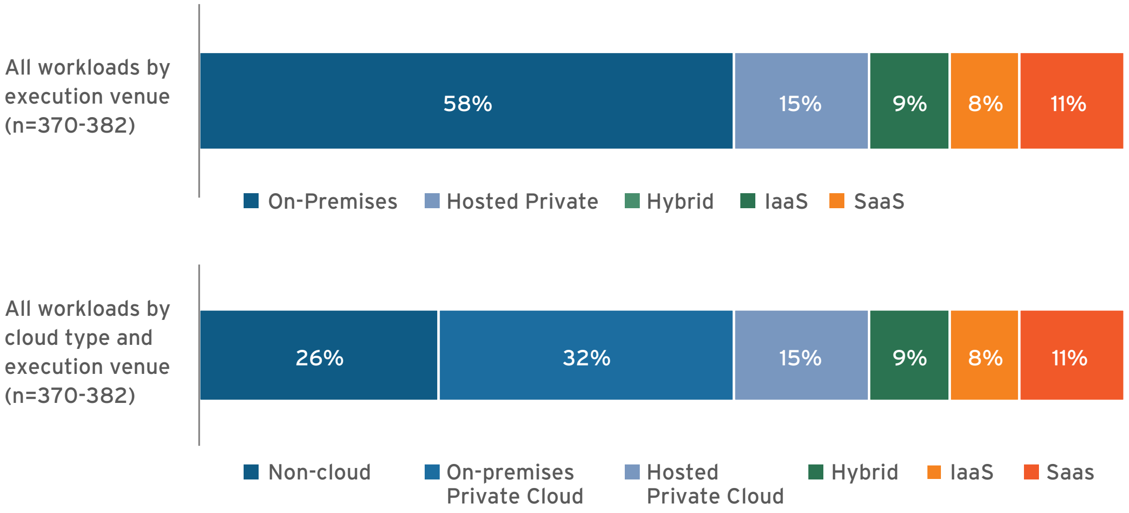
Enterprises have been busy reshaping themselves, embracing the idea that they need to innovate at every level of the business to stay competitive. They need to be responsive to consumer demand that is being reshaped by mobile commerce, and social media requires the integration of technology, analytics and business models. Enterprises have already been embracing cloud services because of the ability to dynamically scale the 'production' of services with demand.

However, a new value chain of production and consumption requires a complete digital infrastructure strategy, meaning a strategy for using all the resources needed to create and deliver new services. Digital infrastructure includes compute capacity, data storage and applications that are orchestrated by policy. This will eventually give rise to a model of service creation in which enterprises are dynamically matching and placing workloads at the best execution venue for a job based on cost, performance, legal and other requirements. In this scenario, the enterprise can use a mix of on-premises private cloud, hosted private cloud and public cloud resources.

End user research provides evidence that enterprises have indeed started down the path to cloud – although most industries are also fairly early on in the journey.

FIGURE 1: WHAT KIND OF CLOUD IS ENTERPRISE USING?

Q: Over the next two years, what will your primary deployment method most likely be for each of the following workloads?



Source: 451 Research's Voice of the Enterprise: Cloud Computing, Q4 2014

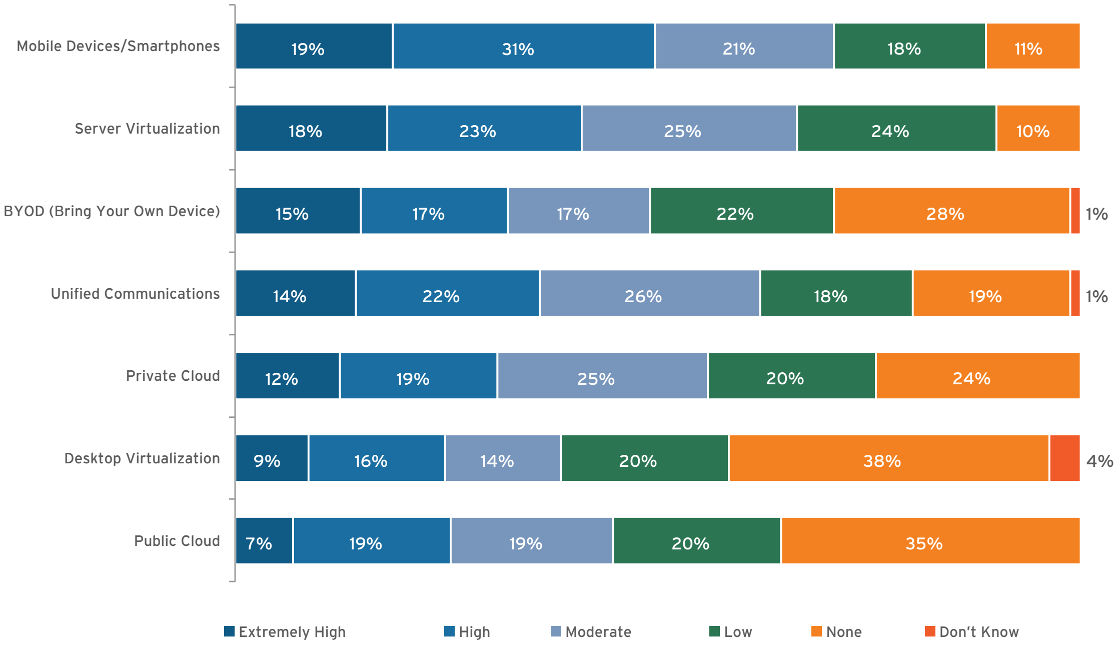
According to our Voice of the Enterprise: Cloud Computing Customer Insight Survey Results and Analysis (Q4 2014), enterprise workloads are anticipated to be mostly on-premises – at least in North America – over the next two years with 58% on-premises, 15% hosted private cloud, and the remaining 28% split between hybrid and public clouds (see Figure 1).

Even given the current state of adoption, hosted private cloud and public cloud are in fact changing enterprise requirements for network performance and availability. In addition to concerns about server virtualization, enterprise IT buyers are concerned about the impact of mobile devices, smartphones and public cloud services on their networks.

In the Wave 11 Networking Survey from TheInfoPro (TIP), a service of 451 Research, 71% of enterprises are saying that mobile computing will have an extremely high, high or moderate effect on capacity and performance over the next 12 months; 56% of respondents say that use of private cloud will do the same, with only slightly less concern registered about the impact of public cloud consumption (see Figure 2).

FIGURE 2: TECHNOLOGIES IMPACTING NETWORK CAPACITY AND PERFORMANCE

Q. For each of the following technologies, please rate the impact on network capacity and performance over the next 12 months.
Please use a 1-5 scale where '1' is none and '5' is extremely high.



Source: 451 Research's TheInfoPro Networking Study – Wave 11

Why are mobile devices such a concern? Applications once entirely internal to an organization are increasingly being accessed from beyond the corporate firewall. Take for example a pharmaceutical company with a large workforce using thousands of devices that are accessing corporate email, applications and product information. Managing device security and application performance across different public networks in a range of different geographic territories becomes quite the challenge.

Compounding performance and capacity issues, the c-suite is battling against internal and external security threats. Whether it's a retailer such as Target, a media company such as Sony Pictures Entertainment or a healthcare provider such as Anthem, the economic fallout and impact on brand equity are examples of the growing cost of security breaches.

The network, the connective fabric for all these resources, needs to be considered a key asset for the digital enterprise. So are private and public IP networks going to be able to perform? Is the Internet secure enough to support the digital enterprise?

2.2 THE CLOUD ADDS SECURITY, PERFORMANCE CHALLENGES FOR ENTERPRISE BUYERS

Whatever the type of cloud in use by an enterprise, it is being viewed as central to achieving the business' goals. When asked about the importance of cloud services in meeting their company's broader business goals over the next two years, 42% of respondents to our Voice of the Enterprise survey rated cloud services as being 'very important' to strategic objectives.

Securing the network would seem to be a top priority, and spending on more security technology would seem like the cure for the problem. Except IT professionals and executives are facing challenges. Here are a few of the concerns from large enterprises (those with revenues of over $1bn annually) expressed during the course of TIP interviews about their budget for network and application security:

Meeting Business Objectives

> *The budget process is broken. If you are the networks tower, you can spend $3-4m a year to maintain and upgrade infrastructure. We don't have a budget to upgrade firewalls, for example. Eighty percent (80%) of the security budget is for staffing.*
>
> *- Large Enterprise, Healthcare/Pharmaceuticals*
>
> *Overall our resource shortage, shortage of people and money. Time and money to keep ahead of attack trends.*
>
> *- Large Enterprise, Consumer Goods/Retail*

Complexity and Risk Management

> *The move to the cloud is a pain point. We have to ensure that the security of the environment we're going to is as secure as the environment within. Trying to get that level of assurance is painful. We do a security risk assessment of the product, then you take it over to procurement and work out those risks with contractual verbiage, but oftentimes the vendor is not willing to make changes to their agreement.*
>
> *Then it gets really complex, with software as a service running on top [of] platform as a service running on infrastructure as a service, all different companies involved, and you ask "If my info is breached, who is responsible?" They all point the finger at each other. No one wants to take responsibility. There's a misconception from business that the cloud is always a better option, cheaper, faster to deploy, rapidly expandable. But they don't realize you still have to manage that space; it's not self- managing.*
>
> *- Large Enterprise, Services: Business/Accounting/Engineering*

Evolving Threat Landscape

> *Constant threat from the dark hole of the... things like the Heartbleed attack, exploitation of deficiency in infrastructure. Always something out there.*
>
> *- Large Enterprise, Financial Services*
>
> *Because the boundaries of the enterprise have morphed into something different, best (security) practices from not too long ago are no longer as effective as they should be.*
>
> *- Large Enterprise, Education*

No wonder, then, that chief information security officers (CISOs) are so busy buying, deploying and trying to integrate an array of security products that over half of the executives surveyed for IBM's 2014 Chief Information Security Officer (CISO) Survey weren't able to look ahead at new security technologies – they're too busy trying to get today's technologies working in concert.

2.3 TECHNOLOGY TRENDS

2.3.1 STRUGGLING TO BOOST SECURITY AND PERFORMANCE TOGETHER

Enterprises want to use the cloud to accelerate business growth. One way to do that is through speeding up the process of making and delivering a good or service. However, increased network performance and improved network security aren't always compatible objectives. One commentator noted:

> *We're always fighting with the business. The business wants things that may make things go faster for them, but it creates security problems.*
>
> *- Large Enterprise, Materials/Chemicals*

Enterprises have traditionally tried to address network performance and security challenges separately. And each piece of the puzzle required using separate pieces of hardware and software: Faster routers, load balancers, application delivery controllers, servers and storage on one hand; new firewalls, intrusion prevention systems and access management systems on the other.

451 Research sees vendors on the path toward combining network and Web application security with content and Web application performance delivered as services, with the potential being that the sometimes opposing goals of increasing both performance and security can both be achieved. At the same time, operational complexity can be (theoretically, at least) simplified by having fewer vendors; also, fewer personnel are needed to manage systems and services, since the vendor does the managing.

This trend is manifesting itself in the marketplace through the combination of content delivery and cloud-based DDoS and WAF services from vendors such as Akamai, Cloud-Flare, Incapsula and Verizon-EdgeCast, for example. But are there indications yet that the enterprise (as well as IaaS and hosting providers) will address its networking security and performance issues in tandem?

For insight into these issues, a look at results from TIP surveys of enterprise end users highlighting spending trends in security is helpful.

SECTION 3

Security Spending Trends

Executives interviewed by 451 Research have clearly indicated that they are adopting a variety of cloud deployment models and allocating more budget to cloud infrastructure. They are moving toward combining network and Web application security. Are customers on board with this notion? Where are enterprises planning to spend their budget?

In 2015, network firewalls are again at the top of the technology list: 31% of security managers are increasing spending according to TIP's Information Security Wave 17 Survey. That number is tied with mobile device management (MDM), where 31% of security managers also report plans for increased spending.

Application-aware or next-generation firewalls (NGFs) round out the top three technologies capturing increased spending in 2015. It is similarly atop our 2014 proprietary Technology Heat Index, a measure of the immediacy of user needs around all tracked security technologies. Palo Alto Networks is the lead in-plan vendor. As commentator interviews indicate, however, application-aware NGFs can be used to defend Web applications against attack, but ultimately, they are to be used in a different battle.

NGFs inspect traffic for malware, but they also control which users can access an application and allow traffic shaping that defines how much bandwidth non-critical applications get. WAFs focus on ways in which the logic of a Web application can be misused by external threats. A WAF models normal Web-app behavior, then blocks external attacks using both a positive (take traffic only from trusted sources) and negative security model.

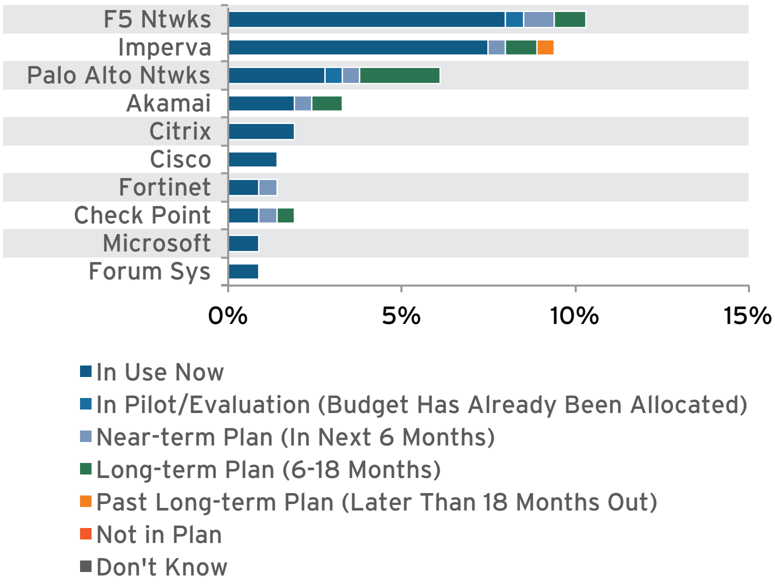
3.1 SPENDING PLANS FOR WAF PRODUCTS AND SERVICES

In our TIP survey results for application security plans, four out of the five top vendors have well-established businesses selling hardware for use in enterprise networks and have also been adding options for running security services on top of VM instances.

WAFs are continuing to benefit from being mentioned in the Payment Card Industry Data Security Standards (PCI DSS) – 5% of security managers in our Wave 17 survey have WAFs in their short-term plans, with another 10% looking at the technology in the longer term.

F5 Networks and Imperva continue to be the leading enterprise choices for WAF offerings (see Figure 3). But Akamai's presence on the list for its WAF service (current deployments, as well as pilot deployments and near-term plans for deployment) suggests there's a growing interest in cloud-based security services.

FIGURE 3: VENDOR IMPLEMENTATION - WAF



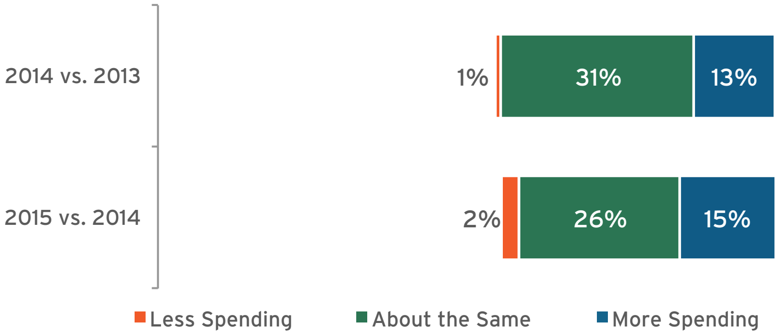
Source: 451 Research's TheInfoPro Information Security Study – Wave 17

The reaction from F5 Networks last year was to acquire a startup called Defense.net, which offered a cloud-based DDoS protection/mitigation service. F5 has recently launched a new hybrid DDoS protection service that leverages the Defense.net technology with F5's on-premises application delivery controllers.

Also in 2014, Imperva acquired the remaining stake in Incapsula that it didn't already own. Incapsula is a provider of WAF and CDN services that started as an independent subsidiary of Imperva.

FIGURE 4: SPENDING CHANGE - WAF

Source: 451 Research's TheInfoPro Information Security Study – Wave 17

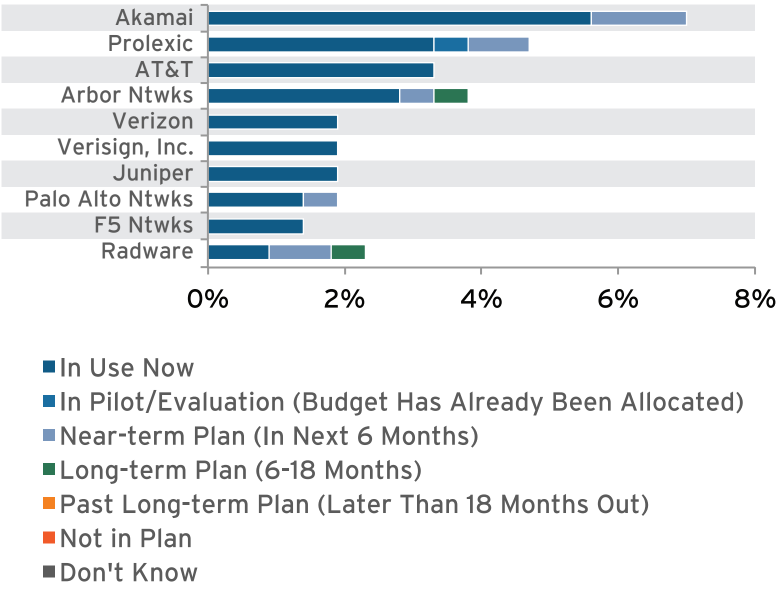


The outlook for spending on WAF technology is that 15% of respondents expect to spend more this year compared to 2014, while 26% say they expect to spend about the same (see Figure 4).

3.2 SPENDING PLANS FOR DDOS PRODUCTS AND SERVICES

DDoS mitigation services score lower on 451 Research's Technology Heat Index map than firewalls, but Akamai/Prolexic are the leading and 'second in use' vendors, with AT&T tied for 'second in use' vendor (see Figure 5). 451 Research's data suggests that enterprises are increasingly interested in DDoS services, but aren't fully in the adoption stage at this point.

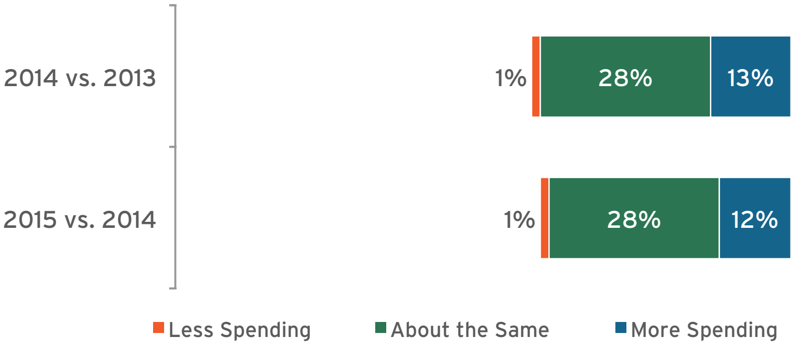
FIGURE 5: VENDOR IMPLEMENTATION - DDOS MITIGATION SERVICES



Source: 451 Research's TheInfoPro Information Security Study – Wave 17

Like Web application defense services, 28% of executives surveyed say spending on DDoS services and equipment will remain about the same, while 12% say spending is likely to increase in 2015 (see Figure 6).

FIGURE 6: SPENDING CHANGE - DDOS SERVICES



Source: 451 Research's TheInfoPro Information Security Study – Wave 17

3.3 ANALYSIS OF WAF AND DDOS SPENDING TRENDS

Given that the complexity and size of DDoS attacks is mostly headed up, there doesn't seem to be as much attention or budget flowing into DDoS and WAF as one might expect – yet. Several factors may be playing into this, including:

- The overall IT budget process in an organization is complex and the buying audience is changing.
- Time and resources are being devoted to other matters such as integrating existing premises-based security solutions.
- WAF technology has a reputation for being hard to manage and can return too many alerts/false positives if rules aren't tuned properly.
- Customers are used to buying hardware for their datacenter, but the systems can't scale to handle the size of current attacks.
- In some cases, technology isn't purchased until an attack has occurred. In other cases, technology is in place, but in the heat of battle it might be found inadequate against an attack.

Regarding budgets for security spending, some of the issues may be related to how companies are organized. Most security teams still report through the IT unit within the enterprise, with 49% of senior security managers reporting to the company's chief information officer (CIO). The CISO remains the top security manager title but it's not clear that CISOs have enough organizational power to effect cultural change within their organizations. Only 24% of CISOs have any manner of budgetary control, and in only a little over half of enterprises (54%) is security a clearly separate division or unit, according to TIP data.

SECTION 4

Drill Down: DDoS Attacks and Mitigation

DDoS protection services are the first nut to crack in the performance and security equation. It's a vexing problem for enterprises that's growing in severity and frequency; it also happens to be the use case where a cloud-based solution presents itself as a very handy solution.

The term 'DDoS' gets used often enough that it may be thought synonymous with high-bandwidth, or 'volumetric,' attacks that are often reported on. The number of attacks reaching over 100Gbps continues to rise, according to various published reports, though by Akamai's reckoning the average peak bandwidth of attacks across its network actually declined from Q3 2014 to Q4 2014 from 13.9Gbps to 6.4Gbps. Apart from the size of volumetric attacks, the last few years have seen a continuous increase in the number of DDoS attacks owing to a combination of factors. These factors include the rise of botnets-for-hire and growing use of attacks using protocols such as SSDP that are used by Universal Plug and Play (UPnP) devices ranging from PCs to printers, routers and mobile devices.

Volumetric DDoS Attacks

Network-based volumetric attacks have the effect of exhausting server resources and/or consuming available bandwidth with spurious requests and/or data. The end result is a denial of service to a legitimate user.

Examples of volumetric attack vectors include User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) and other attacks that flood a network with spoofed requests.

Application-Layer DDoS Attacks

Network-based attacks are still the most common form of DoS attack, but application-based attacks have become more common, and when done in conjunction with a volumetric attack, they can be quite devastating. The purpose of the attack is the same: Deny service to legitimate users by exhausting compute resources. The techniques are different in that the attacker targets Web, application and database resources.

Examples of application layer attacks include Slowloris and vulnerabilities in Web application servers; many zero-day (brand new) exploits fall into this category. These attacks require more sophisticated knowledge of features and vulnerabilities, but can be done without large botnets. These attack types can be harder to detect and harder to mitigate.

4.1 RESPONDING TO ATTACKS

Each attack type has its own options for defense. With volumetric attacks, a variety of solutions can be used, including:

- Addition of bandwidth by the service provider
- Filtering (scrubbing) out bad traffic at the service provider level

- Adding more firewalls and other security devices in the enterprise datacenter
- Using a cloud-based service to filter traffic before ingress into the WAN
- Doing nothing, if downtime is cheaper than the cost of mitigation

Even if downtime doesn't have an immediate impact on revenue, enterprises have their brand reputation at stake, so forgoing any of these mitigation options isn't usually a good choice. That said, protection comes at a price:

- More bandwidth costs money, and might not be needed all the time
- Traffic filtering services can be costly – they work best when 'always on'
- Firewalls and other security devices have limits to their effectiveness
- Scaling on-premises security hardware to potential attacks is untenable
- Hit-and-run attacks will trigger the use of filtering services, but halt after a switchover occurs
- Offsite filtering can be effective, but it takes time to redirect traffic, and some latency is added to the network

4.1.1 USING WAF TO FOCUS ON WEB APPLICATIONS

DDoS-specific solutions are particularly useful for volumetric attacks at the network layer. Many products and services do also have Layer 7 capabilities, but for application-layer attacks, WAFs can integrate with DDoS solutions to provide another layer to the defense that can be justified in several ways.

For one, WAFs protect against known vulnerabilities in widely used applications as well as in-house Web applications. WAFs can do this because they have been designed specifically to examine the contents of the application layer of IP packets. They can function with both a negative (blacklist) security model that blocks known bad actions (usually in the form of pre-defined rule sets as well as rules developed by heuristic algorithms), as well as a whitelist approach that defines what a legitimate request should look like.

Another reason WAFs are being adopted is that they seem on the surface to be a fairly simple approach to bringing Web infrastructure into compliance with PCI standards for protecting Web applications against threats to credit cardholder data. Protecting against unknown vulnerabilities in Web applications is a fine idea, but it shouldn't be misconstrued as an excuse to avoid the use of development practices that incorporate security and quality reviews. Also, the proper deployment and management of WAFs is a significant factor in whether or not they are effective in stopping attacks.

Along those same lines, it is important to note that not all vendors handle DDoS attacks with equal aplomb, nor do all vendors have the same effectiveness with detecting and mitigating application-layer attacks. Available bandwidth, processing power, protocol expertise, data and analytics – all these factors and more play into the effectiveness of an offering. Looking at the basic architecture of a DDoS mitigation solution is one key step toward understanding which approach will work best in a given situation – and help show why the market is moving toward a hybridization of on-premises and cloud-based offerings.

4.2 VENDORS: DDOS MITIGATION

Vendors have a variety of approaches to mitigating attacks. In terms of network architecture, there are vendors that built their businesses around installing hardware at an enterprise or service provider's site but are now adapting to the cloud. Then there are vendors with cloud-based services, as well as telcos and carriers (Verizon, AT&T, Level 3, among others). Enterprise customers often need both, hence a trend toward a hybrid mitigation strategy.

4.2.1 ON-PREMISES MITIGATION

Vendors with devices whose primary purpose is to detect and mitigate DoS attacks fall into this category. While firewalls, IPS devices, application delivery controllers, routers and switches have some defense mechanisms, their performance against DoS attacks falls short of purpose-built systems.

Pros: When used in-line, the protection is always on and is used whenever an attack starts.

Cons: The limit to this approach is that trying to defend against volumetric attacks would require untenable ongoing investments in hardware.

Vendors in this category include (but are not limited to): A10 Networks, Arbor Networks, Corero Networks, F5, Imperva Systems, NSFOCUS and Radware (see Figure 7).

FIGURE 7: SAMPLING OF ON-PREMISES, ANTI-DDOS SYSTEMS VENDORS

VENDOR	PRODUCT	LIMIT (CLAIMED)	TYPES	ARCHITECTURE	COMPETITORS
A10 Networks	Thunder TPS	150Gbps on single system; can scale horizontally to 1Tbps+	Volumetric, protocol, resource, Layer 7	On-premises appliance	Arbor, Corero, F5, Radware
Corero	SmartWall TDS	10-160Gbps	Layers 3-7, volumetric, exhaustion	On-premises appliance	A10 Networks, F5, Radware, RioRey
F5	VIPRION	470Gbps*	Layers 3-7	On-premises appliance	A10 Networks, Arbor Networks, Radware, RioRey
NSFOCUS	ADS Series; WAF Series	Up to 40Gbps	Layers 3/4, Layer 7	On-premises appliance	A10 Networks, Arbor Networks, F5, Radware, RioRey
Radware	DefensePro	300Gbps; can scale horizontally	Layers 3/4, Layer 7, volumetric	On-premises appliance	A10 Networks, Arbor Networks, F5, RioRey

Source: 451 Research, 2015

4.2.2 CLOUD MITIGATION

A cloud-based DDoS mitigation service is, by definition, hosted outside the enterprise datacenter. Vendors will typically have several points of presence (called scrubbing centers) that ingest traffic bound for the customer, mitigate attacks and send clean traffic on its way to the customer.

Pros: Offers the advantages of on-premises gear (in-line, always on) but can offer greater scale to defend against volumetric attacks. It is essentially a managed service that doesn't require additional personnel to manage.

Cons: These services can be deployed in always-on fashion, but for cost reasons are often deployed only when an attack has been detected. This can result in delays in defending against attacks.

Vendors in this category include (but are not limited to): Akamai (Prolexic), Black Lotus, CloudFlare, Incapsula, Level 3, Neustar and Verisign (see Figure 8).

FIGURE 8: SAMPLING OF CLOUD-BASED DDOS PROTECTION SERVICES VENDORS

VENDOR	PRODUCT	LIMIT (CLAIMED)	TYPES	ARCHITECTURE	COMPETITORS
Akamai	Kona Site Defender	10+Tbps (mitigation bandwidth)	Layer 7, volumetric	Redirect scrubbing	CloudFlare, Imperva
Akamai	Prolexic	2.8Tbps+	Layers 3/4, Layer 7	Cloud DDoS mitigation	Verisign, Neustar
CloudFlare	Advanced DDoS Protection	400Gbps (NTP)	Layers 3/4, DNS, SMURF, ACK, Layer 7	Redirect scrubbing	Akamai, Imperva, Zscalar
CDNetworks	Cloud DDoS protection	NA	Layers 3/4, DNS, volumetric, Layer 7	Cloud-based	Akamai
Imperva	Incapsula	1Tbps mitigation/ scrubbing	Layers 3/4, DNS, volumetric, Layer 7	Redirect scrubbing	CloudFlare, Akamai, Yottaa
Level 3	DDoS mitigation service	4.5Tbps ingest/ scrubbing	Layers 3/4, Layer 7 (basic), exhaustion, volumetric	Cloud-based	AT&T, Verizon, Verisign, CloudFlare
Verizon-EdgeCast	DDoS mitigation service	NA	Layers 3/4, Layer 7	Cloud DDoS mitigation	AT&T, Level 3

Source: 451 Research, 2015

Technology vendors with on-premises offerings also typically have carrier-grade services with higher bandwidth and mitigation capacity that are being sold to carriers, telcos and cloud and hosting providers; this equipment is then used to build a DDoS mitigation service.

Cloud IaaS providers, for instance, are primarily interested in protecting their network infrastructure so their end customers aren't getting taken out by a DDoS attack aimed at them, but expect to see attack mitigation and other security services increasingly being offered as a value-add offering to cloud and hosting services.

4.2.3 HYBRID MITIGATION

This describes the combination of on-premises equipment owned by an enterprise (for example) with additional protection from a cloud-based service. In one scenario, a hybrid service takes the form of a managed service provider managing customer hardware and redirecting traffic to scrubbing centers when necessary.

Pros: Ideally, a hybrid solution means on-premises equipment and cloud services are fully integrated and automated.

Cons: Pricing can still be out of reach for smaller enterprises.

Developments are occurring rapidly in this area (see Figure 9). For example:

- Arbor Networks sells its Arbor Cloud service to enterprises using Arbor's Peakflow and Pravail systems. Arbor sells the service to large enterprises directly, but companies that want a fully managed service can contract with partner Neustar.
- F5 acquired Defense.net in 2014 as its cloud-based system and has integrated the renamed Silverline DDoS Protection service with its on-premises hardware.
- Imperva Systems now wholly owns Incapsula, which was previously an independent subsidiary that offered a CDN and DDoS protection service.
- Radware last year introduced a cloud-based DDoS protection service for enterprises that integrates with its on-premises equipment to deliver single-vendor hybrid protection; it also sells carrier-class versions of its DefensePro mitigation device to service providers that are using the equipment to build their own cloud-based DDoS mitigation service. Integration with Cisco's Application Centric Infrastructure (ACI) fabric could pave the way for service providers and SDN-minded enterprises invested in Cisco to add cloud-based DDoS services in the near future.

It's not just hardware vendors that want to link up with cloud providers; the reverse holds true as well. Verisign's cloud-based DDoS service can be integrated with on-premises security devices via a recently released API.

FIGURE 9: SAMPLING OF HYBRID ON-PREMISES/CLOUD DDOS PROTECTION VENDORS/PARTNERS

VENDOR	PRODUCT	LIMIT (CLAIMED)	TYPES	ARCHITECTURE	COMPETITORS
A10 Networks	Thunder TPS	150Gbps on single system; can scale horizontally to 1Tbps+	Volumetric, protocol, resource, Layer 7	On-premises appliance/virtual appliance/cloud architecture for third-party services	Arbor, Corero, F5, Radware
Arbor Networks	Arbor Cloud	10Gbps	Layer 7, exhaustion, volumetric	Cloud/proxy-based Neustar for managed service	F5, Verisign
Black Lotus	DDoS protection	1Tbps	Layers 3/4, Layer 7	Cloud/Huawei for on-premises	CloudFlare, Incapsula
Corero	SmartWall TDS	10-160Gbps	Layers 3-7, volumetric, exhaustion	On-premises appliance/ cloud provider partnerships in process	A10 Networks, F5, Radware, RioRey
F5 (Defense.net)	Silverline Ready Defense	2Tbps mitigation/1Tbps scrubbing	Layers 3/4, DNS, volumetric, Layer 7	Cloud-based/ on-premises appliance	Verisign, Akamai
F5 (Defense.net)	Silverline Always Available	8Tbps	Layers 3/4, DNS, volumetric, Layer 7	Redirect scrubbing/ on premises appliance	Verisign, Akamai, Radware, Arbor
Imperva	Incapsula	1Tbps mitigation/ scrubbing	Layers 3/4, DNS, volumetric, Layer 7	Redirect scrubbing	CloudFlare, Akamai, Yottaa
Neustar	SiteProtect	1Tbps	Layers 3/4, Layer 7	Cloud/Arbor for on-premises	Verisign, Akamai
NSFOCUS	ADS Series; WAF Series	Up to 40Gbps	Layers 3/4, Layer 7	On-premises appliance; Black Lotus for cloud-based services	A10 Networks, Corero, F5, Radware, RioRey
Radware	DefensePipe	Over 1Tbps	Layers 3/4, Layer 7, volumetric, SSL, DNS	Cloud-based/hybrid integration with Cisco ACI fabric	Arbor, CloudFlare, Neustar
Verisign	DDoS Protection Services	NA	Layers 3-7	Cloud/hybrid [1]	Akamai, Neustar
Verizon	DoS Defense	NA	Layers 3/4, Layer 7	Redirect scrubbing (on-net); Arbor Cloud for off net	AT&T, Level 3

1: Via partnership with Juniper Networks; other appliances can signal via an open API

Source: 451 Research, 2015

SECTION 5

CDN: Adding Performance Back to the Cloud

There's no arguing that WAF and DDoS services can be worth their weight in gold when a business is under attack. However, having DDoS protection always online can be expensive, and properly tuning WAF filters can be time-consuming for staff. Apart from operational costs, there is a performance cost to security services. That in turn leads to a potential lost sale. In e-commerce, for example, a number of studies have shown that consumers generally expect a mobile site to load as fast as a site on a desktop computer. In 2011, consumers would wait five seconds before abandoning a mobile site; now some reports put that figure between two to three seconds. The equation is simple: faster page load times equate with more opportunities to show ads and sell stuff.

How to recoup the time spent making the network and application more secure? Technologies long deployed in CDNs are one way to improve performance for applications delivered from the cloud. A CDN does this by using compute, storage and network resources to place content such as files or other objects close to an end user for improved performance.

For dynamic content, CDN services use IP and TCP-level protocol optimizations to deliver objects to the user more quickly. Most CDNs now also offer content optimization as a component of their service, which affects page load times by re-ordering the delivery of content (or in some instances, such as a slow wireless network, by blocking the loading of third-party content and scripts), re-sizing images and compressing JavaScript and images.

Another trend has more CDN providers incorporating real-user measurement data into decisions about how and when to deliver different components of the Web page. Some CDNs can act like a hyper-distributed compute cloud by executing a customer's application logic on the CDN's servers. The combination of caching, acceleration and compute services can improve the performance and availability of cloud-based services.

A growing number of vendors offer both CDN and security services in tandem, with varying levels of integration (see Figure 10).

FIGURE 10: SAMPLING OF CDN VENDORS OFFERING DDOS AND WAF SERVICES

VENDOR	PRODUCT	ARCHITECTURE	WAF?
Akamai	Kona Site Defender	Redirect scrubbing	Yes
Akamai	Prolexic	Cloud DDoS Mitigation	No
CloudFlare	Advanced DDoS Protection	Redirect scrubbing	Yes
CDNetworks	Cloud DDoS Protection	Cloud-based	No
Imperva	Incapsula	Redirect scrubbing	Yes
Instart Logic	ProxyWall	Reverse proxy	Yes
Level 3	DDoS mitigation service	Cloud-based	No
Verizon-EdgeCast	DDoS Mitigation service	Cloud DDoS mitigation	Yes
Yottaa	Cloud Firewall	Cloud-based	Yes

It should be noted that vendors such as Alert Logic, Fireblade, Radware, Sucuri and Qualys offer a cloud-based WAF service and could provide services in tandem with a CDN vendor. Fireblade, for example, integrates its WAF technology with Verizon-EdgeCast CDN for content delivery.

5.1 ADDING ANOTHER LAYER FOR A MULTILAYERED APPROACH TO SECURITY

Independent of a traffic inspection and scrubbing service that the CDN service provider might offer, the architecture of CDNs offers an added measure of protection against volumetric DDoS attacks. A CDN maps requests for content to a localized point of presence; an attack against a website doesn't go directly to that website, instead hitting the CDN first. A CDN's larger number of points of presence and servers makes it harder to bring down the origin site, with its more limited bandwidth and server power.

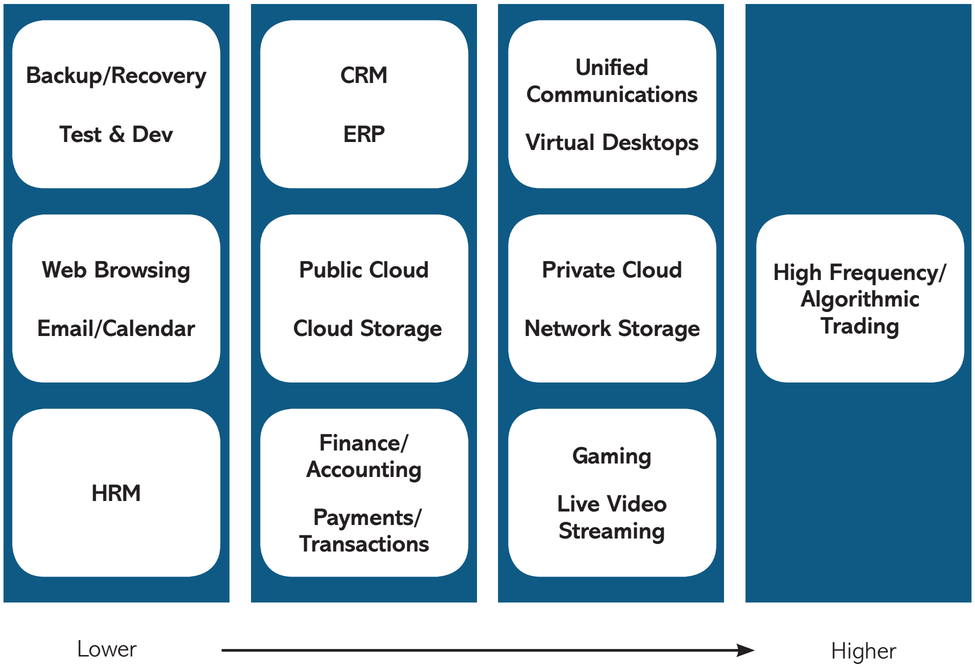
Other services, variously referred to by names such as origin shield or site shield, also point the way toward a further security measure: Hide the entire infrastructure behind the CDN. By 'going dark,' an enterprise reduces its attack surface because it is only communicating directly with the CDN's servers.

5.2 A CDN FOR EVERY APPLICATION?

Does every application protected by a WAF and/or DDoS mitigation service benefit from use of a CDN? The availability of an application (and the security of data) is of utmost importance to all enterprises, but not all enterprises have (or perceive) a need for performance.

Figure 11 offers an illustration of some typical applications and an estimate of their sensitivity to network latency. (We exclude latency introduced within the datacenter and application infrastructure.)

FIGURE 11: SENSITIVITY TO NETWORK-BASED LATENCY, BY APPLICATION TYPE



Backup/Recovery Test & Dev	CRM ERP	Unified Communications Virtual Desktops	
Web Browsing Email/Calendar	Public Cloud Cloud Storage	Private Cloud Network Storage	High Frequency/ Algorithmic Trading
HRM	Finance/ Accounting Payments/ Transactions	Gaming Live Video Streaming	

Source: Interxion, Nokia, 451 Research

Some applications can benefit more than others from a CDN. At the high-performance (i.e., low-latency) end of the market, trading and other financial services functions have gravitated toward specialized network services and datacenter providers able to provide close proximity to major trading platforms such as the New York Stock Exchange. This isn't an area where CDNs have an impact. Instead, market verticals where vendors with content delivery and cloud-based security services should be the first targets.

Gaming and video streaming, for instance, are two markets that already commonly use one (or more) CDNs. Due to the revenue associated with these services, they are increasingly using security services to protect their businesses.

Private cloud and network storage are harder cases to make for CDN use, at least where a CDN only delivers content over public IP networks. That's one reason why Akamai has partnered with Cisco to incorporate its software in Cisco's networking gear. Other vendors license their software for use in creating 'enterprise' CDNs that move traffic along private networks. There is a growing trend to blend use of private and public cloud, and there is a role for CDNs to accelerate applications and content (and protect them) in that use case. Any market where there is a move toward a SaaS delivery model, including CRM, ERP and HRM, has potential for CDN vendors.

It should also be noted that providers of cloud services have both performance and security reasons to partner with companies that offer CDN and DDoS and other security services.

At the least, a public cloud provider has to protect its infrastructure for the common good. A site or its associated components running on a provider such as Amazon Web Services (AWS) or Rackspace that is being hit with a DDoS attack runs the danger of draining bandwidth from other customers in a multi-tenant environment. While the cloud providers listed in Figure 12 have mainly focused on selling content delivery and acceleration services, there is clearly a growing opportunity to sell the DDoS and WAF offerings of their CDN partners.

FIGURE 12: CLOUD PROVIDERS ALIGNING WITH CDNS

CLOUD SERVICE PROVIDER	CDN PLATFORM	LICENSING OR RESELLING
Amazon.com	Internal development (CloudFront)	NA
AT&T	Akamai	Reselling
HP	Akamai	Reselling
KDDI	CDNetworks	Licensing
Korea Telecom	Akamai	Reselling/Managed CDN
LeaseWeb	Internal development	NA
Media Temple	EdgeCast, CloudFlare	Reselling
Microsoft	Internal development/ EdgeCast Networks	Reselling
NTT	Verizon/EdgeCast	Licensing
Orange	Akamai	Reselling/Managed CDN
Rackspace	Akamai	Reselling
SoftLayer (IBM)	EdgeCast	Reselling
Swisscom	Akamai	Reselling/Managed CDN
Telefónica	Akamai/Internal development	Reselling
Telus	EdgeCast	Licensing
Verizon	EdgeCast	Acquired

Source: 451 Research, 2015

SECTION 6

Conclusions & Recommendations

The 'enterprise' isn't just a collection of employees working in a building, connecting to the Internet from a PC that is behind a firewall. The enterprise is already moving toward a scenario in which employees use wireless mobile devices to access multi-tenant cloud SaaS services such as Salesforce.com. In this scenario, the enterprise manages part of the network. Yet, there is still a need for the functions (visibility, control, security, performance assurance, compliance) the enterprise network provides.

The increasing reliance on both private and public IP networks for services will eventually result in the functions of the enterprise network also being provided by cloud services. Security services will be delivered on demand, and have the ability to rapidly scale in response to attacks that might overwhelm traditional premises-based security solutions. CDN resources at the edge of the network are well placed to act as a first line of defense against attacks, and can also help improve application performance.

CDN vendors aren't the only providers of cloud-based security and performance solutions; traditional security vendors are also fortifying their offerings with cloud services that do defense work beyond the perimeter of the enterprise datacenter. Network service providers (carriers, telcos and ISPs) and IaaS providers are also seeking to augment enterprise security with cloud-based services.

6.1 RECOMMENDATIONS FOR END USERS

- In general, addressing issues such as giving CISOs more budgetary control and aligning IT and security units to a common vision are steps that will help ensure projects succeed.
- Consider ways to augment protection from DDoS attacks at all layers by using cloud-based detection and mitigation services.
- Give priority to those vendors with a roadmap for integration with on-premises equipment, if vendors have not already implemented APIs.
- Enterprises with significant revenue from Web operations (e.g., e-commerce, online gaming) should consider placing Web infrastructure behind a CDN provider to increase protection from DDoS attacks.

6.2 RECOMMENDATIONS FOR VENDORS

- For hardware vendors, easier integration between on-premises and cloud-based services will be a big key in making inroads with enterprise customers. Don't just send more alarms; leverage existing alerting tools to improve attack mitigation.
- For CDN vendors, focus on market verticals such as SaaS providers, gaming, online content and enterprise-oriented applications such as collaboration, virtual desktop infrastructure (VDI) and salesforce mobility as areas that will benefit most from reduced latency. Offering DDoS mitigation and WAF services separate from content delivery can be a way to get a foot in the door of enterprises that aren't yet convinced they need performance from a CDN.
- Security vendors that have been selling gear to service providers and are now also offering their own cloud-based service will need to craft a channel strategy that minimizes conflict with existing customers. Enterprise revenue may not make up for lost sales to telcos and carriers in the near term.

6.3 RECOMMENDATIONS FOR SERVICE PROVIDERS

- Network service providers (carriers, telcos and the like) need to consider partnering with vendors of DDoS mitigation services if they can't provide off-net services. Larger enterprises will almost invariably have some security needs that will be out of region; help simplify procurement and operations for your customer by having a strategy already in place.
- Cloud service providers have already moved toward offering CDN services, often in partnership with a third-party service provider. Consider extending these practices to the security offerings these partners may have, or consider whether your vendors for datacenter security (DDoS, firewall, WAF, etc.) have a strategy for extending capacity via their own cloud.
- Leverage operational analytics across your entire infrastructure – what data can be integrated with a DDoS or WAF service for purposes of improving protection of your clients, or for service orchestration, for instance?

GLOSSARY

Technology Heat Index: Measures user demand for a technology based on several factors including usage or planned usage, changes in planned spending, an organization's budget for the relevant IT sector and future changes in the organization's budget. A high score means a technology is expected to see significant growth.

Technology Adoption Index: Measures aggregate investment in a technology based on several factors including usage or planned usage, changes in planned spending and an organization's budget for the relevant IT sector. A high score means the technology is already experiencing healthy adoption.

INDEX OF COMPANIES